The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies (U)

Michael Schwartzbeck

> **"In the last year, several academic, commercial, and free speech advocates have seriously jeopardized the US Government's legal right to control encryption."**

Encryption technology has long been an important and closely guarded tool for military, diplomatic, and government missions. Nations depend on encryption to commuoicate private information across the world and through "enemy" territory; without encryption, any nation's most valued secrets are easily comptomised. History books attest to the value the Allies placed on the broken German and Japanese encryption systems during World War II. It is with this sense of worth that the United States guards its encryption capahilities and it efforts to decrypt other countries' communications. For decades, the US Government has monopolized encryption and decryption efforts, capabilities, and research. In recent years, however, the information revolution has begun to challenge this monopoly with some success. In rhe last year, several academic, commercial, and ftee speech advocates have seriously jeopardized the US Government's legal tight to control encryption.

An Early Challenge

On 24 Octobet 1952, Ptesident Truman signed a top secret presidential memorandum[1] that consolidated many of the service and national cryptological functions into the National Securirty Agency (NSA). Since then, NSA has been tasked with protecting and advancing America's cryptologic capabilities. Fot decades, NSA has had several mechanisms designed to limit the public discussion of cryptologic tesearch. O[redacted]method was to embrace corporate and educational teseatch labs and think tanks through organizations such as the National Securiry Agency Scientific Advisory Board (NSASAB).

Through the NSASAB, senior NSA scientists historically met with leading industry and university mathematicians and scientists to discuss the cryptologic applications of emerging theories in science and technology.[2] While NSA officials had a true interest in attracting the brightest thinkers in the United States, they also used the NSASAB as a tool to bring cryptology's leading thinkers into association with NSA and thus be able to classify their work, which then removed it ftom the public vision and the eyes of foreign cryptological services.

Another similat project was the creation in 1958 of the Communications Research Division (CRD) within the Institute for Defense Analysis. The CRD was a private, independent think tank dedicated to helping NSA solve advanced cryptologic problems. Co-located at Ptinceton University's John von Neumann Hall and a site near the Pentagon, the CRD has been led by such cryptological luminaries as Dr. [redacted] a professor of mathematics at Cornell University; [redacted] a mathematician with both the Sandia Corporation and the University of Illinois; and Dt. [redacted] the chairman of the Universiry of Chicago's mathematics department.

Michael Schwartzbeck is at the National Imagery and Mapping Agency.

(b)(3)(c)

(b)(3)-P.L. 86-36

The CRD regularly welcomed the nation's brightest thinkers. Their work at CRD was heavily classified, however, and no CRD research has ever been published in the open press.[3]

The union of compartmented postgtaduate reseatch and NSA sponsorship was disrupted in the late 1960s by the introduction into the universitry environment of affordable computer technology and corporate financial interests. During that time, IBM board chairman Thomas Watson, Jr., ser up a cryptology reseatch group that developed a cipher (codenamed Lucifer) for use in a cash-dispensing system that IBM had heen developing.[4] At first, the Lucifer ciphet was not very sophisricated, but, with the help of Carl Meyer, a German-born elecrrical engineer with a doctorate from the University of Pennsylvania, IBM retooled the ciphet a number of times; in 1974, it was teady for the market. This ciphet had a key that was 128 bits long, significantly longer rhan the keys of any other publicly developed encryprion programs available to the public at the time.[5]

This incredibly long cipher key led many to believe that the Lucifer code would be rruly unbreakable, even by NSA's standards. For the first time in its history, NSA's decryption capabilities were seriously threatened by public reseatch, and the agency quickly moved to rectify the situation.

> **"For the first time in its history, NSA's decryption capabilities were seriously threatened by public research, and the agency quickly moved to rectify the situation."**

This action effectively demonstrated that "strong" cryptography was srill controlled by the government and not available for public sector use. Unfortunately for NSA, rhis did not solve their problem. The NSA/IBM key-length agreement was widely publicized, and many public teseatchers felt thar the NSA was unfairly stifling their work for secretive, and possihly ulterior, reasons. Many protests were lodged, and a vatiety of public cryptographic rcsearch groups emerged throughout educational and corpotate centers in response.

The Information Revolution and Changing Contexts

This disagreement between Intelligence Community (IC) cryptographers and public researchers simmeted until the late 1980s, when the information revolurion first began to be felt. As interconnecrivity and computer rechnology began to increase exponentially, the Internet began to grow in popularity, and telecommunications, business practices, and international political realities changed dramatically. New issues develnped concerning rhe Glnbal and National Information Infrastructures, global electronic commerce, legal jurisdictions, and intelligence requirements, including:[6]

- *US defense and intelligence needs evolved.* There has been considerable debate on the IC's roles, missions, and resources. Public perception of government needs changed with greater interests in counternarcotics, terrorism, transnationalism, and economic issues.
- *Encryption needs proliferated, especially for nongovernment and nonmilitary purposes.* Businesses and individuals created legitimate needs fot "strong" encryption. Increasing needs for an electronic means to transfer funds, send and receive data, and conduct commerce over intra- and internets led to a greater need for strong encryption.
- *Expertise in encryption was no longer found only in the military and in the government.* Computer software and hardware firms and academic institutinns began producing high-quality encryptinn codes. Many businesscs exist for rhe sole purpose of creating strong encryprion for business purposes.
- *Encryption capabilities became dependent on computer software and hardware.* This led to a greater union between encryption and industry, with all sectors being transformed by the growth of computer technologies.
- *Strong cryptography became widely available.* Both inside the United States and abroad, encryption software has come to he widely marketed.[7] Even if no US-originated cryprography products are ever exported, it will still proliferate worldwide.
- *The information revolution changed business practices, concepts of government sovereignty, and the way the*

(b)(1)

(b)(1)
(b3)-18 USC 798, P.L. 86-36

(b)(1)
(b)(3) 18 USC 798; P.L. 86-36

world is viewed. To a significanr degree, the trust thar most citizens placed in theit governments and their willingness to defet to government authotity ate gone.

- *Computers are now viewed as contributing significantly to the expansion of personal freedoms such as free speech.* Many see encryption as a critically importanr method of protecting personal privacy on computer networks. Many also use computet networks extensively for their ptivate business and personal communications needs.

- *Traditional definitions of intellectual property became questionable.* Information no longer has to be prinred or made available through newsstands, bookshops, and libraries ro be widely circulated.

- *"Product cycles" in computer software, hardware, and telecommunications industries became considerably shorter than government "policy cycles."* Timelines for research, development, production, and marketing of new technologies are much shorter than timelines for government's implemenration of new policies. Ponderous govemment approaches are seen as increasingly illogical and unwarranted.

These issues led public and government cryptoanalysts to feel a need to revisit the issue of government conttol of cryptography. The Clinton administration understood the changing role of cryptography and tried to address these issues early on. Its first attempt came in April 1993 with the "Clipper chip." The chip was to be installed in all US-produced computers, and it depended on a key escrow[8] account that would allow the govetnment to hold copies of every key in use by the public, so it could decrypt any message ir felt necessary. Even though the administration promised strict control of the decryption keys,[9] including storage and warehousing by a disinterested third parry, ptivacy groups complained of an Orwellian plot. AT&T was the only major corpotation to sign up for the chip, in a move that its management discovered to be a tremendous error. The Clipper chip was recognized as a failure that would never be accepted by corporate America, and the Clinton administration stopped pushing it.

Next, the Clinton administration suggested that the encryption industry adopt the NSA-approved Digital Encryption Standard (DES) and Digital Signarure Standard (DSS)[10] for its encryption needs. The administration wanted DES and DSS to be the standard, all-purpose encryption programs fot all public and corporate needs. The largest encryprion keys that DES and DSS could use were 56 bits long, and critics complained that 56-bit keys were not strong enough. Besides, critics argued thar for NSA to endotse any code, it had to be able to decrypt it on a regular basis. Again, NSA was portrayed as "Big Brother."

Exportation Issue Reveals a Need For Change

The major changes in technology and encryprion were illustrared by one US software encryption company when ir decided to export its strong encryption code internationally. RSA Dara Security was founded in 1979 by three scientists at Massachusetts Institute of Technology, who had created and parented a strong encryption program. For a long time, their code was too complex for available computet technologies. By 1987, however, the computer industry had caught up to RSA and the company began signing contracts with Lotus, Motorola, Apple, and others. But their biggest controversy came in 1991,[11] when RSA Data Security tried to market its program to Microsoft, which then wanted to integrate the code into its programs to be marketed at home and abroad.

RSA landed the contract with Microsoft. MasterCard, Visa, and other large financial institutions later announced specifications fot Internet financial transactions based on RSA encryprion.

This proliferation of RSA's strong code was disconcerting to NSA's cryptoanalysts. NSA feated that if this program was made commercially available and widely disseminated, it would no longer be able to collect, analyze, and produce communications intelligence.[12]

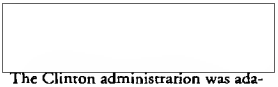
NSA felt that if the people it targets were to get this software, they could communicate electronically without any feat being monitored.

The Arms Export Control Act (AECA) of 1976 and the Intetnational Trade in Arms Regulations (ITAR), tevised 1992,[13] severely restrict US companies from exporting

(b)(1)
(b)(3) 18 USC 798; P.L. 86-36

any and all military and intelligence-related technologies. During the Cold War, most aspects of encryption technology, including the hardware, software, and the mathematical algorithms on which cryptography is based, were classified as military technologies and placed on AECA's "Munitions List." This same list is used to prohibit the export of tanks, fighter jets, and aircraft carriers.

The Department of State had statutory responsibility for administering the AECA and ITAR regulations, which it managed through the Office of Defense Trade Controls (ODTC). Any US corporation wishing to export a technology on the AECA Munitions List was required to submit an export license application to the ODTC, which would then pass the application to the government agency best qualified to decide whether the technology should be exportable or not. ODTC always passed encryption export applications to NSA for review, and any code too strong was denied an export license.



The Clinton administration was adamant that US companies would not be allowed to export strong encryption.[14]

Bidzos and RSA were not yet done. Bidzos realized that there was a simple way to skirt the export limitation laws.

Both the AECA and the ITAR are US laws, and, as such, they only pertain only to US companies. Bidzos went to Japan and established a Japanese subsidiary, Nihon RSA.[15] Nihon RSA qualified as a distinct Japanese company, subject only to Japanese law, and Bidzos was able to do whatever he wanted with his strong encryption technologies.[16] Knowing that his encryption technology was a desired commodity, he shopped it around the Japanese marketplace. He promptly struck a deal to produce encryption chips for Nippon Telephone and Telegraph Corporation.

> **"The Clinton administration was adamant that US companies would not be allowed to export strong encryption."**

Others Enter the Exportation Fray

At about the same time NSA and the Clinton administration were losing the battle with RSA and Jim Bidzos, several other public sector cryptographers were beginning to find success in propagating strong cryptography. In the early 1990s, a cryptographer named Philip Zimmetman created PGP (for Pretty Good Protection), data-encryption software that scrambles e-mail messages. PGP is a strong encryption program; 1,024-bit keys are common in this program.[17] Because PGP is a strong program, it fell under AECA and ITAR export control guidelines. Before the US Government could place controls on it, however, the PGP software appeared on the Internet as shareware.[18] Placing PGP on the Internet made it available worldwide to anybody with a computer and a modem,[19] so it had in effect been exported without the prior approval of the US State Department.

Although several other encryption programs were already available on the Internet, users from around the world began downloading PGP; the program became very popular and well respected among Internet users. The US Department of Justice was not pleased with the disregard for US export regulations, and it decided to prosecute Philip Zimmerman. Unfortunately for the Department's case, it could not link Zimmerman to the software website on the Internet, and, in 1996, Zimmerman was acquitted of any wrongdoing.[20] This court case was viewed by many as a major victory for the public use and availability of strong encryption.

Another case occurred in February 1995, when the Electronic Frontier Foundation (EFF) sued the US Government on behalf of Daniel Bernstein. The EFF charged that the Federal government was violating Bernstein's First Amendment rights by stifling the research he did as a graduate student at the University of California at Berkeley in strong cryptography. As with the PGP case, Bernstein was trying to publish his research papers and place his encryption software, known as Snuffle 5.0, on the Internet, and the government was citing his disregard for AECA and ITAR regulations. In January 1997, Judge Marilyn Patel ruled in favor of Bernstein,[21] on the grounds that AECA and ITAR violated the free-speech guarantees of the Constitution.

Before long, three separate bills were on the floor of Congress, each guaranteeing the right of Americans to use or sell any encryption they wanted domestically and eliminating export controls on any free or mass-market commercial encryption programs.[22] These separate bills were

(b)(1)
(b)(3) 18 USC 798; P.L. 86-36

introduced by Senator Conrad Burns, Reptesentative Bob Goodlatte, and Senator Parrick Leahy; the Goodlatte and Leahy bills would have also made it a Federal crime ro use encryption to conceal the commission of a felony. Senator Robert Dole co-sponsored the Senate bills, charging that "the administration's big brother proposal will literally destroy America's computer industry."[23] Leahy stated, "These bills are pro-privacy, pro-jobs, and pro-business." While none of these bills became law, they did attract the attention of the media. Government control of strong cryptography quickly became a controversial and popular topic in the media.

Players and the Issues

By this time, each of the major interest groups in this debate had come out with compelling arguments for their own cases and similarly strong arguments denouncing opposing viewpoints.[24] The groups can be summarized as follows:

- *NSA cryptoanalysts.* NSA's stake in this argument has been its desire to continue to be able to carry out its primary mission. NSA analysrs have stated that the proliferation of strong encryption has severely degraded their ability to collect intelligence. (b)(3)(n) Sophisticated nonstate actors, such as terrorist cells and drug cartels, will be even hatder to track.

- *Public researchers.* This group's main arguments have been the preservation of free speech and the right to continue to do scholarly research. The US courts have shown that the free speech argument has some validity.

> **"The lines of battle were generally drawn with NSA and law enforcement officials on one side and public researchers and corporate investors on the other."**

- *Corporate investors.* Investors have been looking for a way to ensure that electronic money transactions can be done with a high degree of confidence. Without strong encryption, consumers will not place their trust in electronic transfers, and systems like the Intemet will never reach their business potential.

- *Law enforcement officials.* If strong encryption becomes available to the world's criminals, this group will not be able to gather evidence and track criminals to prevenr crimes; this group also fears that its ability to fulfill its duties will be degraded, with serious impact on public safety.

The lines of battle were generally drawn with NSA and law enforcement officials on one side and public researchers and corporate investors on the other. Public researchers and corporate invesrors complained that the US Government was still operating with a Cold War mentality, despite the fact that Cold War patadigms have been replaced; they claimed that any organization as secrerive and manipularive as NSA had no place in a free and democratic society. In their eyes, US citizens should have the right ro communicate privately, without any fear of government eavesdropping, and they believe free and private speech can only be guaranteed with strong encryprion. Bruce Scheier, directot of the Intemational Association for Cryptographic Research, also pointed out rhat, "The ability to publish is required in any vibrant academic discipline."[25]

Business leaders emphasized that electronic financial transactions will only be reliable and safe from tampering when strong encryption is used. And encryption software writers complained about the business opportunities they were missing: the estimated US data encryption market grew from $384 million in 1991 to $946 million in 1996. Worldwide rotals are believed to have been $695 million in 1991 and $1.8 billion in 1996.[26] The software industry estimared that, if export controls were removed, US companies could sell as much as $60 billion a year[27] in encryprion hardware and sofrware by 2000.

On the other hand, law enforcement concerns generally paralleled NSA's in rhat strong encryption would give wrongdoers impenetrable communications that would allow them to operate undetected. As more strong encryption programs become available, more groups will acquire and use encryption, and, even if the US Government is able to crack those codes, it will be at a much greater expense, particularly in costs of computer time.[28] Many in the government have also felr that the "free and private speech" argument was disingenuous; as retired Vice Admiral McConnell, vice president of Booz-Allen & Hamilton and former NSA director, charged, "Those who argue in this arena usually have an agenda. Often when they are arguing one set of conditions, they will be using the privacy argument when what they ate really trying ro do is sell software encryption."[29]

The National Research Council Report

By now, the Clinton administration realized that its encryption policies were not effective and were not addressing the pertinent issues of the debate. Its Clipper chip had failed, its DES and DSS encryption standards were similarly unsuccessful, and the exportation rules were disliked and increasingly ineffective in stopping the spread of strong encryption. President Clinton responded by asking the National Research Council to do a study on the various arguments for and against US export controls on strong cryptography. The 20 members of the panel represented a wide variety of interests, and they included Kenneth Dam of the University of Chicago Law School, Bruce McConnell of the Office of Budget and Management, former Attorney General Benjamin Civiletti, former deputy director of NSA Ann Caracristi, and Council on Foreign Relations President Leslie Gelb.[30] Their 500-page report, "Cryptography's Role In Securing the Information Society," or CRISIS,[31] was finished in June 1996, and it was highly critical of the Clinton administration's position.

The report concluded that using arms control laws to regulate encryption "is not adequate to support the information security requirements of an information society."[32] The authors also believed that the broad outlines of a national cryptography policy could be analyzed in an unclassified environment and that export control restrictions should be "progressively relaxed but not eliminated." The panel also noted that the plan to introduce escrowed encryption keys was not without merit, but that it was "relatively untried and entails its own potential risks."[33]

The panel's consensus was that "widespread commercial and private use cryprography is inevitable in the long run and...its advantages, on balance, outweigh its disadvantages."[34] One benefit of adopting this policy, the panel noted, is that US companies could start putting much stronger encryption programs in their software, which would allow US citizens to have an increased standard of cryptographic protection. The panel's final conclusion was that government encryption policies should be examined in the same light as other US economic regulations.

The Administration Moves

The administration did not take long to respond to the National Research Council's recommendations. On 15 November 1996, President Clinton released Executive Order 13206: "Administration of Export Controls on Encryption Products." In this Executive Order, Clinton followed many of the recommendations of the CRISIS report; most important, he took cryptographic hardware, software, and technologies off of the AECA Munitions List and placed them under the statutory responsibility of the US Department of Commerce. Specifically, management of encryption fell under the regulations guiding "dual-use" (both military and civilian) commodities outlined in the Export Administration Act of 1979.[35] This move greatly eased the government controls on public use and exportation of strong crypotography. The only major requirement for exportation was a key escrow system. The resulting differences in the old and new encryption policy are listed below:[36]

"Clipper Chip" Era Policy (February 1994)

- *Hardware implementation:* Clipper chip required in each piece of US software.
- *Algorithm classification:* Secret.
- *Maximum key length:* 40-bits.
- *Decryption keys held by:* US Government.
- *Decryption keys held:* For all crypto, both domestic or internationally exported.
- *Keys available to:* Law enforcement and intelligence agencies.
- Exported strong crypto requires key recovery.
- No limit on domestic use of cryptography.

Newer, Revised Policy (October 1996)

- *Algorithm classification:* Unclassified.
- *Maximum key length:* Unlimited, if keys are recoverable when requested.
- *Decryption keys held by:* Corporate third parties following government guidelines.
- *Decryption keys held:* Only for exported crypto with keys 56 bits or longer.
- *Keys available to:* Law enforcement and intelligence agencies.

- Exported strong crypto requires key recovery.

- No limit on domestic use of cryptography.

This major shift in policy was met with increased enthusiasm from the public sector as well as the government. Vice President Gore said, "This initiative will make it easier for Americans to use stronger encryption products—whether at home or abroad."[37] Robert Holleyman, President of the Business Software Alliance, was also impressed, calling the plan "forward progress."[38] Stephen Walker, CEO of Trusted Information Systems, likened the policy change to "imagining during the Cold War that the Berlin Wall would fall."[39] A few others were not so impressed: Senator Conrad Burns stated, "This debate is not over by any stretch of the imagination."[40]

Encryption Key Recovery

Although some public researchers and corporate investors were still leery of the key escrow mandate, most of the groups involved in this debate accepted the escrow requirement, which was one of President Clinton's major requirements for this easing of encryption regulations. The administration has given industry a two-year grace period, at the end of which there will need to be a viable key recovery system in place and operating. Many large companies have backed the escrow system; Dorothy Denning, a cryptography expert from Georgetown University, lauded it as a useful way to recover keys "necessary to unscramble important data left by a deceased, departed, or unethical employee."[41] That the escrow accounts would be held by a trusted third party in the corporate world eased many of the "Big Brother is watching" concerns. More important, keys will only be given to the US Government in response to warrants or court orders. To show its support, IBM has teamed up with Apple, Digital, Groupe Bull, Hewlett-Packard, NCR, Sun, Trusted Information Systems, and even RSA Data Security[42] to develop an interoperable key-recovery industry standard. RSA's James Bidzos conceded, "We are seeing the market move to emergency access [of keys]."[43] Soon after, America Online, Compaq, Motorola, Novell, Northern Telecom, and 29 others joined in escrow discussions, which has strengthened the industry alliance.[44]

Detractors of the key escrow system are led by Victor Parra, president and CEO of the 550-member Electronic Messaging Association (EMA). Parra is frustrated that keys have to be held by third parties; he feels that employees of the user company are the only key holders that can really be trusted. Parra notes that e-mail and Internet transactions will tend to be limited to domestic firms, because international trading partners will be uneasy with a third party having escrow access. EMA has also noted that the two-hour limit to turn over requested keys is unreasonable, and many software makers have agreed that encryption software prices will rise as a result of escrow requirements.[45]

Escrow Goes International

William Reinsch, the Undersecretary for Export Administration at the US Department of Commerce, wants the policy to move beyond US borders and create a worldwide standard for key escrow. Reinsch theorizes that, if escrow becomes pervasive and institutionalized in international commerce, terrorists and criminals will be forced to submit to key recovery systems.[46] This would also help prevent US companies from relocating overseas to avoid current US escrow requirements.

The European Commission is considering an encryption industry standard for key recovery similar to the one proposed by the Clinton administration, and, if implemented, all codes used throughout Europe would require a trusted third party to hold a copy of the key. IBM supports the new US and European escrow proposals; to those US firms that oppose the move, they state, "We would prefer that they take a more global focus."[47] Another group, a consortium called Eurobit-ITAC-ITI-JEIDA, comprised of major Canadian, European, Japanese, and US business firms, has called for the harmonization of regulations on the export, import, re-export, and use of cryptography. Their goal is to develop a set of principles that, "reach consensus on issues which need to be treated at the worldwide level."[48]

International support does seem to be growing. Representatives from the nations of the Organization for Economic Cooperation and Development (OECD) backed the concept of key recovery systems[49] during a January 1997 conference. The OECD emphasized that information security is an international matter because information systems cross national boundaries. At a separate RSA Data Security-sponsored conference, David Aaron, US Special

Envoy to the OECD, stated that important US allies support President Clinton's position that governments should be able to recover encryption keys when necessary. He also added that he had discussed cryptography issues with representatives of France, the UK, Germany, Belgium, and Canada.

The Future of Strong Encryption

The Clinton administration has made a serious, if belated, effort to meet the evolving encryption needs of US citizens and industries. It was quick to notice and act on the outdated Cold War standards of Department of Defense control on encryption technologies and algorithms. After several false starts, the administration has produced a policy that goes a long way toward meeting the requirements of four diverse and often diametrically opposed groups: public researchers, corporate investors, law enforcement officials, and intelligence analysts.

The US Government, and NSA in particular, would like to return to the Cold War era of complete government control over strong cryptography and skillful manipulation of the research and corporate communities. But strong encryption has proliferated beyond US Government control. A failure to make any concessions to the changing times would have been disastrous for the Clinton administration's relationship with US business and free speech communities. It would also have crippled US software encryption companies trying to compete with overseas companies not shackled by restrictive regulations. And, even if the administration could keep strong encryption out of US industry, it would still proliferate; other nations around the world are just as likely to create strong codes.

So, acknowledging that strong encryption regulations needed to be addressed, the administration took the safest possible route by initiating a series of limited reforms aimed at pleasing all parties while continuing to meet intelligence and security needs. The Clipper chip, DES, DSS, and the key escrow system were each successive attempts to produce a policy that would meet the burgeoning needs of US business and free speech communities without forgetting the critical requirements of the law enforcement and intelligence communities.

What is next? Obviously, an international resolution on the control and management of encryption technologies is a desirable goal, if not a lofty one. Critics of the Clinton administration are right in noting that sophisticated criminals and terrorists will not use the encryption systems that require key escrow registration. If an international referendum requires all encryption systems and users to register their keys, however, then criminals and terrorists will be forced into the escrow system. A worldwide key escrow system will not be put into place quickly, but with serious effort it may be attainable, and it is a worthwhile goal. The proliferation of strong encryption is already beyond control, but perhaps the continued monitoring of criminals and terrorists is not.

NOTES

1. James Bamford, *The Puzzle Palace: Inside The National Security Agency, America's Most Secret Intelligence Organization* (New York: Penguin Books, 1983), p. 80.
2. *Ibid.*, p. 247.
3. *Ibid.*, pp. 430-433.
4. *Ibid.*, pp. 434-435.
5. A passage from *The Puzzle Palace* (p. 438) accurately relates the importance of the length of a key to a code's strength:

   "How long it takes to break a code depends on the length of the key. For a 56-bit key, the number of possible combinations would be about 70 quadrillion. By using a computer with a million special-purpose chips, capable of testing 2 trillion possible keys per second, the entire range of keys could be searched in 70,000 seconds—or less than 20 hours [with most solutions found within 10 hours]....

   Then there is the matter of cost. According to two Stanford scientists, the chips themselves could be produced for about $10.00 each, or $10 million altogether...[the entire computer] could be built for about $20 million.... The daily operating cost would be about $10,000 a day, meaning that each solution would cost about $5,000.

   [With the 128-bit key,] the results would have been dramatically different. As opposed to the moderate $5,000 price tag, each solution would cost an unimaginable $200 septillion, or $200,000,000,000,000,000,000,000,000,000,."

   The general principle is that the longer the length of the key, measured in bits, the more difficult it is to crack the code.
6. Stuart J. D. Schwartzstein, "Export Controls On Encryption Technologies," *SAIS Review*, (winter 1996), pp. 17-21.
7. For a review of several commercially available encryption software pro-

grams see: Jay Munro, "Psst! Keep A Secret?" *PC Magazine* 15, (17 December 1996), pp. 45-50.

8. An encryption key "unlocks" or decrypts a coded message.

9. Steve Levy, "Scated Bidess," *Newsweek* 127, (10 June 1996), p. 50.

10. David Stipp, "Techno-Hero or Public Enemy?" *Fortune* 134, (11 November 1996), pp. 178-180.

11. *Ibid.*, p. 180.

12. *Ibid.*, pp. 180-182.

13. Schwartzstein, pp. 15-16.

14. Ivars Petetson, "Boosting Cryptography's Role in Security," *Science News* 149, (8 June 1996), p. 357.

15. Tim Beardsley, "For Your Eyes Only?" *Scientific American* 275, (September 1996), p. 44.

16. The US Department of Justice confirmed this loopbole by choosing not to prosecute Bidzos.

17. David L. Wilson, "Pretty Good Privacy: Software Is a Popular tool for Encrypting Messages," *Chronicle of Higher Education* 43, (13 September 1996), pp. A28-A29.

18. Shareware is software openly available on the Internet for public use at no cost.

19. PGP is srill available on the Internet at <<http://web.mit.edu/network/pgp.html>>

20. Wilson, "Pretty Good Privacy...," p. A28.

21. David L. Wilson, Karla Haworth, and Andrew Mytelka, "Federal Judge Strikes Down Government Restrictions On Computer encryption," *Chronicle of Higher Education* 43, (10 January 1997), p. A24.

22. Rick Henderson, "Know The Code," *Reason 28*, (June 1996), p. 16.

23. Levy, p. 50.

24. Robert K. Acherman, "Security Balances Needs of Privacy, Law Enfotcement," *Signal* 51, (Februaty 1997), p. 23.

25. Wilson, Haworth, and Mytelka, p. A24.

26. Schwartzstein, p. 14.

27. Henderson, p. 16.

28. Schwartzstein, p. 26.

29. Acherman, p. 23.

30. Elizabeth Koch, "Confronting A Crisis: Clipping Clinton's Enctyption Policies," *Reason* 28, (November 1996), p. 22.

31. This repott can be found on the Internet at http://www.nap.edu/readingroom/books/crisis.

32. Koch, p. 22.

33. Peterson, p. 357.

34. Levy, p. 50.

35. Schwartzstein, p. 16.

36. Gary H. Anthes, "Feds Ease Crypto Rules, But With a 'Key' Catch," *Computerworld* 30, (7 October 1966), p. 32.

37. Anthes, "Feds Ease...," p. 32.

38. *Ibid.* p. 32.

39. John Carey, "Big Breakthrough--or Big Brother?" *Business Week* 3502, (18 November 1996), pp. 88-90.

40. *Ibid*, pp. *88-90.*

41. Anthes, *"Feds Ease...,"* p. 32.

42. Lynda Radosevich, "HP Pushes Encryption Scheme," *Infoworld* 18, (25 November 1966), p. 9.

43. Carey, p. 90.

44. Marthew Woolacort, "Vendors Coalesce on Encryption," *Infoworld* 18, (23/30 December 1966), p. 39.

45. Barb Cole, "Encryption Conniption," *Computerworld* 31, (6 January 1997), p. 3.

46. Gary H. Anrhes, "Encryption Policies Srill Under Fire," *Computerworld* 30, (9 Decembet 1996), p. 74.

47. Graeme Browning, "Anothet Federal Code to Crack," *National Journal* 29, (11 January 1997), p. 89.

48. Schwartzstein, p. 30.

49. John Markoff, "A Consensus Is Sought On Coding," *The New York Times*, (29 January 1997), p. D-19.